

2024年2月19日
株式会社ベッセルホテル開発
(ベッセルイン心齋橋)

【重要なお知らせ】

不正アクセスを原因とするフィッシングサイトへの 誘導ショートメッセージの配信について

ベッセルイン心齋橋（大阪府中央区。以下「当ホテル」といいます。）におきまして、当ホテルにおいて利用している Booking.com 社の管理画面が不正アクセス者による不正アクセスを受け、同社経由で当ホテルをご予約いただきました一部のお客様に対し、フィッシングサイト（実在の宅配業者や金融機関、ショッピングサイトなどを装った偽のサイトで、アカウント・ID やパスワード、クレジットカード番号などの個人情報を入力させ騙し取るために設けられたサイト。）へ誘導するショートメッセージ（以下「誘導ショートメッセージ」といいます。）が配信されてしまいました。お客様には多大なるご迷惑とご心配をおかけしておりますこと、深くお詫び申し上げます。

つきましては、調査により判明しました事実につきまして、次のとおりご報告いたします。

第1 原因について

Booking.com 社および関係機関と連携し、原因の究明や被害の内容等について調査を進めてまいりました。

その結果、当ホテルにおいてシステムを管理する弊社端末のうち1台がマルウェア（悪意のあるソフトウェアの総称）に感染し、不正アクセス者によって窃取された認証情報が使用され、当ホテルで利用する Booking.com 社の管理画面に不正アクセスされたと判断しております。

第2 被害結果について

1 誘導ショートメッセージの配信について

(1) 不正アクセス者による行為態様

Booking.com 社の調査の結果、不正アクセス者は、宿泊予約者の個人情報にはアクセスすることなく、予約を行った宿泊予約者に対し、誘導ショートメッセージを自動応答設定により送信したことが判明しました。

(2) 誘導ショートメッセージが配信された期間

2024年1月11日

(3) 誘導ショートメッセージが配信されたお客様

Booking.com 経由で下記期間を宿泊日としてご予約をいただきましたお客様
2024年1月12日～2024年11月22日（98名）

第2 個人情報の漏えい又は流出の有無

今回の不正アクセスによるお客様の個人情報の漏えい又は流出は確認できませんでした。

第3 クレジットカード情報について

Booking.com 社より、クレジットカード情報を閲覧された形跡はなかったとの報告を受けております。

第4 誘導ショートメッセージへの対応とお願い

1 弊社の対応

(1) 誘導ショートメッセージが配信されたお客様への対応

当ホテル又は Booking.com 社から同内容の注意喚起のご連絡を差しあげております。

(2) 弊社に直接お問い合わせいただきましたお客様への対応

状況をご説明のうえ、記載された URL リンクへアクセスしないようご案内しております。

2 お客様へのお願い

(1) 全てのお客様へ

引き続き不審なショートメッセージにご注意ください。

不審なショートメッセージを受信されたときは、貼付された URL のリンク先へアクセスしないようお願い申し上げます。

(2) リンク先にアクセスし、クレジットカード情報の入力や支払いを行ってしまったお客様へ直ちに Booking.com 社へのご連絡をお願いいたします。

第5 今後の対応と再発防止策

調査結果及び関係機関等からの指摘を踏まえ、予約管理システムのパスワード変更及び、従業員に対する教育等を実施しました。

今後も引き続き、更なる対策の強化を行ってまいります。

以上